DEFENSE SECURITY COOPERATION AGENCY
201 12TH STREET SOUTH, SUITE 101
ARLINGTON, VA 22202-5408

JUL 07 2021

MEMORANDUM FOR DEFENSE PRIVACY, CIVIL LIBERTIES, AND TRANSPARENCY DIVISION

SUBJECT: Justification for the Use of the Social Security Number for the Defense Security Cooperation University Information System – Mission, *DIPTR ID #16274*

This memorandum justifies the collection and continued use of the Social Security Number (SSN) within the Defense Security Cooperation University (DSCU) Information System - Mission (DISM) pursuant to the acceptable use categories, *Legacy Interface System* and *Operational Necessity*, established in Department of Defense Instruction 1000.30, "Reduction of Social Security Number (SSN) Use Within DoD," Incorporating Change 1, Effective April 15, 2020.

The DSCU is a subordinate organization of the Defense Security Cooperation Agency (DSCA) that provides professional research, education, and training of U.S. Government security cooperation and security assistance programs for DoD, U.S. Defense Industry, international military, and related government civilians globally. DSCU utilizes DISM, an internet-based portal, to collect and use supplied information, including the SSN, for the purposes of efficient administration of both U.S. and international students, including the effective management of personnel and guest lecturers.

Further, DISM utilizes the DSCU Web system (*DIPTR ID #15640*) on MilCloud to collect student information, when applicable. The SSN, along with other PII, is transmitted through DSCU Web which serves as an entry point for student training data only. DSCU Web does not store or retrieve the student training data. The information is transferred into DISM, at which point it is removed from DSCU Web.

DISM interacts with the Defense Travel System (DTS) which requires the continued use of the SSN as a primary identifier for DoD military and civilian personnel who travel nationally and internationally. Subsequently, DTS interfaces with the Defense Finance and Accounting Services (DFAS), which further relies solely on the collection of the SSN for reimbursement of travel expenses. To enable DSCU to properly fund requests for reimbursements of approximately 2,000 students per year, the process mandates the use of the traveling student's full SSN. Note, DSCU cannot access a student's information within DTS when they are not a part of the DSCU organization, nor can individuals outside of the organization access the DSCU account within DTS without the setup of a cross-org funding source. Using the SSN, the budget office creates the cross-organization funding source within DTS for the TDY student. As a result, the student is able to view and charge necessary traveling expenses to DSCU's line of accounting. Upon receipt of the order number for the student's travel expenses, the SSN is subsequently deleted from DISM.

In addition, DSCU collects the SSN for guest speakers in order to fulfill Internal Revenue Service requirements to identify the individual by the Tax ID (SSN) for reimbursement of the honorarium. The SSN is also required for non-DoD speakers who are traveling to DSCU and need a user's profile set up in DTS to reimburse the guest speaker's travel expenses.

While we await guidance from the Department regarding DoD-wide migration from the use of the SSN for the preparation of government travel and related matters, DSCU currently uses best industry practices and a DoD Risk Management framework to ensure the SSN, along with other personal data within DISM, is not misused outside of the correct context of the system. Further, the data is stored in an encrypted format in an encrypted database which requires PKI-authentication for access. The data is maintained in a controlled facility. Physical entry is restricted by the use of locks, and is accessible only to authorized personnel. Access to records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for need-to-know. Access to computerized data is restricted by centralized access control to include the use of Common Access Cards, passwords (which are changed periodically), file permissions, and audit logs.

Additional information regarding DISM's data collection can be found in the published System of Records Notice (SORN) and Privacy Impact Assessment (PIA) located on DSCA's public website at https://www.dsca.mil/about-dsca/privacy-act-program.

Heidi H. Grant
Director